DATE

**SECURITY ADVISORY FOR
AFFECTED OPERATING POWER REACTOR LICENSEE
AND FUEL CYCLE FACILITIES**

(SA-0x-xx)

SUBJECT: USE OF AUTHENTICATION CODES TO VALIDATE CALLER IDENTIFICATION DURING IMMINENT THREATS AND PHYSICAL ATTACKS

The U.S. Nuclear Regulatory Commission (NRC) has identified the need to expedite the verification of caller identity in the case of an imminent threat to a nuclear power plant (NPP) or fuel cycle facility (FCF). This is specifically important in the case of an imminent airborne threat.

The current process of verification (verification protocol) is as follows: NRC receives threat information from an external source (e.g., the North American Aerospace Defense Command and the U.S. Northern Command (NORAD/NORTHCOM)) and telephones the licensee. In order to verify that the caller is actually the NRC, the licensee has two options: (1) While the receiver of the call stays on the line, another member of the licensees' staff can call the NRC Operations Center to verify the authenticity of the call; and (2) The receiver of the original call can hang up the phone and call the NRC Operations Center back to perform the verification. This process is performed similarly if the licensee calls the NRC Operations Center to notify an imminent or actual security threat.

The current verification protocol requires resources that would be better dedicated to other tasks such as notifying additional State and local first responders. Additionally, this protocol could delay licensees' actions in an imminent threat response environment. In light of these issues, NRC will use authentication codes with our licensees to verify a caller's identity whenever a caller notifies an imminent threat. The use of these codes will provide a short, simple means of call authentication that will eliminate the need to perform a call back and still maintain reasonable assurance of the caller's identity.

Proposed Authentication Code Process

On a daily basis, NRC will generate and provide a random 4-digit alphanumeric sequence to each main control room during the daily plant status communications check (4:00 AM). The codes will go into effect each day at 8:00 AM Eastern Standard/Daylight Time (ESDT). In the unlikely event of an imminent threat notification prior to 8:00 AM ESDT, NRC and the licensee

will use the currently in effect code (i.e., the code that NRC-provided the previous day) to authenticate the caller.

NRC has not classified the authentication code as safeguards information. NRC has deemed not classifying the code to be an acceptable risk when balanced by the short lifespan (24 hours) and limited distribution of each daily code and the simplified handling of the information. Although NRC issues only one code at a time, not in sets of a week's or month's worth, NRC still will distribute the authentication code to licensee staff on a "need-to-know" basis to minimize the possibility of caller deception or call "spoofing."

Each licensee should develop a process for maintaining the authentication code in a convenient, accessible location to prevent delaying the transfer of information during imminent threat report communications.

Call Process

The call process of reporting an imminent threat from the NRC Operations Center to an affected licensee is described below.

1. NRC Headquarters Operations Officer (HOO) calls the affected licensee.

2. When the licensee picks up the phone, the HOO will indicate the origin and purpose of the call and state that the HOO is ready to authenticate.

3. The licensee will respond when ready for authentication.

4. The HOO then will provide the current authentication code.

5. The licensee will verify that the correct code was given.

6. If the correct code was given, the HOO can pass the information to the licensee without further verification.

7. If the incorrect code was given, the licensee will call back the NRC. No code word will be utilized for the call back.

Example Exchange During an Imminent Threat Report

An example of the expected exchange during an imminent threat report is shown below.

NRC HOO: " This is the NRC Operations Officer, I have NORAD on the line with potential threat information, I am ready to authenticate."

Licensee: "Go ahead NRC."

NRC HOO: "The authentication code is Charlie November Eight Zulu."

Licensee: "That is correct. Go ahead NRC."

This process is similar to NRC's requirements for a prompt notification (within 15 minutes) by the licensee of an onsite security threat. The report is made, and the authentication code is provided to the NRC Operations Center allowing additional notifications to other Federal organizations (e.g., Department of Homeland Security (DHS)).

Implementation of Authentication Code Process

NRC expects to have this process in place 3 months (12 weeks) after the issuance of this advisory notice. Licensees are responsible for developing procedures and training applicable personnel in this process. This is not meant to encumber the licensees with additional requirements, and licensees are encouraged to keep the process as simple as possible.

The NRC HOOs will coordinate and perform pilot phone calls with licensees during the implementation period. These calls will ensure that the process is working and efficient prior to full-scale implementation.

Paperwork Reduction Act Statement: The information collections contained in this Safeguards Advisory are covered by the requirements of 10 CFR Part 50, which were approved by the Office of Management and Budget, approval number 3150-0011.

Public Protection Notification

NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

Approved by _____

William F. Kane
Deputy Executive Director for Reactor
and Preparedness Programs
Office of the Executive Director